INSTITUTE FOR DEFENSE ANALYSES

# NSD-4943
# The Common Risk Model for Dams: A Portfolio Approach to Security Risk Assessments

Yev Kirpichevsky
Yazmin Seda-Sanabria, U.S. Army Corps of Engineers
Enrique E. Matheu, U.S. Department of Homeland Security
Jason A. Dechant
M. Anthony Fainberg
J. Darrell Morgeson
Victor A. Utgoff

June 2013

Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, Virginia  22311-1882

Approved for public release;
distribution is unlimited.
IDA Log No. H 13-000889

**About This Publication**

The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

**Copyright Notice**

4850 Mark Center Drive, Alexandria, Virginia 22311-1882 • (703) 845-2000.

NSD-4943

# The Common Risk Model for Dams: A Portfolio Approach to Security Risk Assessments

Yev Kirpichevsky
Yazmin Seda-Sanabria, U.S. Army Corps of Engineers
Enrique E. Matheu, U.S. Department of Homeland Security
Jason A. Dechant
M. Anthony Fainberg
J. Darrell Morgeson
Victor A. Utgoff

June 2013

# A portfolio approach to security risk assessments

Y. Seda-Sanabria, US Army Corps of Engineers, USA
E.E. Matheu, Department of Homeland Security, USA
J.D. Morgeson, Y. Kirpichevsky, M.A. Fainberg, J.A. Dechant and V. Utgoff, Institute for Defense Analysis, USA

**The Common Risk Model for Dams (CRM-D), described here, was developed as a result of collaboration between the US Army Corps of Engineers and the US Department of Homeland Security. It is used for security risk assessment of dams, navigation locks, hydro projects, and similar infrastructure. The method provides a systematic approach for evaluating and comparing security risks across a large portfolio. Risk is calculated for attack scenarios (specific adversary using a specific attack vector against a specific target) by combining consequence, vulnerability, and threat estimates in a way that accounts for the relationships among these variables. The CRM-D can effectively quantify the benefits of implementing a particular risk mitigation strategy and, consequently, enable return-on-investment analyses for multiple mitigation options across a large portfolio.**

In 2005, the Institute for Defense Analyses (IDA) initiated the development of the Common Risk Model (CRM) for evaluating and comparing risks associated with the nation's critical infrastructure. This model incorporates commonly used risk metrics that are designed to be transparent, simple, and mathematically justifiable. The model also enables comparisons of calculated risks to assets and systems within and across critical infrastructure sectors.

A modified version of this model has been under development by IDA in collaboration with the US Army Corps of Engineers (USACE) and the US Department of Homeland Security (DHS). The modified model, the Common Risk Model for Dams (CRM-D), takes into account the unique features of dams and navigation locks, and provides a systematic approach for evaluating and comparing risks from adaptive threats across a large portfolio [Seda-Sanabria *et al.*, 2011[1]].

At the most basic level, risk is estimated for an attack scenario, defined as:

- a specific adversary (for example, a highly-capable transnational terrorist group);
- a specific target (for example, the main impoundment structure of a specific dam); and,
- a specific attack vector (for example, a cargo van loaded with explosives).

Risk is defined as the expected value of loss and is a function of three variables: threat (T), vulnerability (V), and consequences (C):

$$R = f\,(T, V, C) \qquad \text{... (1)}$$

Threat is defined as the probability of an attack scenario being attempted by the adversary, given the attack on one of the targets in the portfolio under assessment, or P(A); vulnerability, as the probability of defeating the target's defences, given that the attack is attempted, or P(S|A); and, consequences, as the expected consequences of the attack, given that the target's defences are defeated, C. Because of the way in which CRM-D estimates these three variables, it is appropriate to calculate risk as their product:

$$R = P(A) \times P(S|A) \times C^{(*)} \qquad \text{... (2)}$$

CRM-D also defines 'conditional risk', or $R_C$, as risk for the attack scenario, given that this scenario is chosen$^{(**)}$:

$$R_C = P(S|A) \times C \qquad \text{... (3)}$$

The consequence and risk metrics currently considered in the CRM-D are loss of life and total economic impacts. The sum of risks for all the attack scenarios under consideration is termed 'portfolio risk'. Minimizing portfolio risk, subject to available resources, is often the focus of risk managers.

## Fundamental concepts of CRM-D

The CRM-D methodology integrates the outputs of three separate models: consequences (external to CRM-D), vulnerability, and threat. Using modelling is a natural choice for estimating the outcomes of complex physical and economic processes, such as consequences from attack, but is equally important for estimating vulnerability and threat, that is, variables which require more subjective input from subject matter experts (SMEs). This is because there are many possible attack scenarios, and the set is continuously changing. It is prohibitively costly and time-consuming to elicit expert judgements on vulnerability and threat for every scenario, and to repeat the elicitation process every time a new scenario is introduced or old scenarios are modified. This makes modelling crucial when developing risk estimates in support of return on investment (ROI) analyses, because the impacts on risk of potential risk-mitigation improvements need to be assessed quickly.

The vulnerability and threat models are based on data elicited from SMEs in a way that makes it possible to apply elicited SME judgement to any set of attack scenarios. The elicitations were conducted for estimating risk from highly capable, transnational adversary groups. Elicitations in support of estimating risk from other types of adversary are currently under develop-

*The functional relationships among the variables are accounted for by estimating P(A) as a function of the other two variables, but there is no stochastic relationship because P(S|A) and expected consequences are estimated as point values, and not random variables. This justifies the use of the product function [Cox, 2008[2]].

**Note that the risk metric in Eq. 2 is also conditional on the attack within a portfolio under assessment. The "conditional risk" metric is further conditioned on the particular attack being chosen.

ment. Because the adversaries' capabilities and/or intent are likely to change with time, elicitations should be repeated every few years or as deemed appropriate.

## Vulnerability

To evaluate the vulnerability of a target to a specific attack by a specific adversary, a model of layered defences is adopted. The defensive layers protecting a given target could potentially include national defences (for example, national counter-terrorism activities), local defences (for example, local law enforcement capabilities to detect and respond to potential attacks), and target defences (for example, on-site security systems and protective measures). The methodology for producing vulnerability estimates accounting for target defensive layers is described in detail by Seda-Sanabria *et al*. [2011[3]]. The methodology for producing vulnerability estimates for national and local defensive layers is currently under development.

In CRM-D, an attack is considered 'successful' if every defensive layer is breached successfully, and the attack reaches the target. Therefore, for the conceptual attack scenario shown in Fig. 1, P(S|A) can be determined using the following expression:

$$P(S|A) = P(B1|A) \times P(B2|B1) \times P(B3|B2,B1) \qquad \dots (4)$$

where: P(B1|A) is the probability of successfully breaching the first layer given the specific attacker under consideration attempts this attack; P(B2|B1) is the probability of successfully breaching the second layer given that the attacker has successfully breached the first layer; and, P(B3|B2,B1) is the probability of successfully breaching the third layer given that the attacker has successfully breached the first and the second layers.

Each layer is defined by its defensive attributes. For a national defensive layer, these can be the characteristics of relevant programmes and activities implemented at the national scale, such as the security screening conducted at airports; for a local defensive layer, these can be the level of participation in intelligence information-sharing of local law enforcement agencies and their prevention/response capabilities; and for the target defensive layers, these can be the characteristics of site security measures, such as vehicle barriers, access control systems, security force, and so on.

Regarding target defensive layers, there is a relatively small number of combinations of defensive attributes that are typically implemented on dams and related facilities. These commonly used configurations are called layer-defensive configurations, or LDCs. Because of the small number of LDCs, it is feasible to elicit probabilities of success for each reference attack vector against each LDC for each type of attacker under consideration. The vulnerability estimate for a given LDC reflects subject-matter expert (SME) judgement on how the defensive attributes of that LDC would perform against a particular attacker using a particular attack vector, based on the attacker's capabilities and intent and the attack vector's characteristics.

Probabilities of success against individual LDCs are combined into a P(S|A) for a scenario as shown in Eq. 4. The probability of success against a layer is conditional on which layers have already been breached, since some layers can degrade attackers' capabilities in various ways. Further, P(S|A) incorporates the possibility that some layers may or may not be encountered (for example, response forces may or may not arrive in time to engage the adversary before the attack succeeds). The process of estimating P(S|A) in light of these factors is discussed in detail by Morgeson *et al*. [2013[4]].

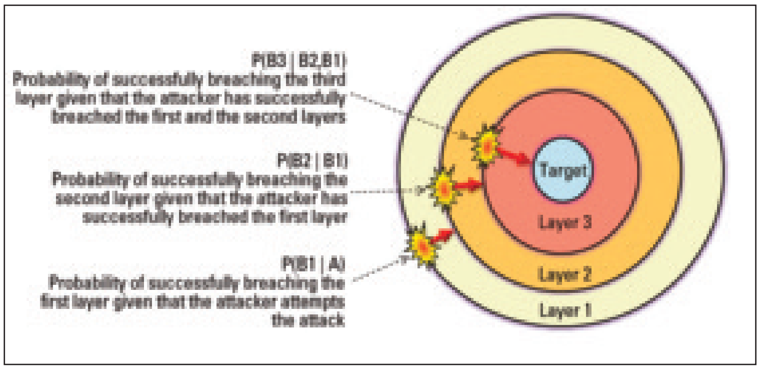

P(B3 | B2,B1)
Probability of successfully breaching the third layer given that the attacker has successfully breached the first and the second layers
P(B2 | B1)
Probability of successfully breaching the second layer given that the attacker has successfully breached the first layer
P(B1 | A)
Probability of successfully breaching the first layer given that the attacker attempts the attack
Target
Layer 3
Layer 2
Layer 1

*Fig. 1. Conceptual model of layered defences.*

### Threat

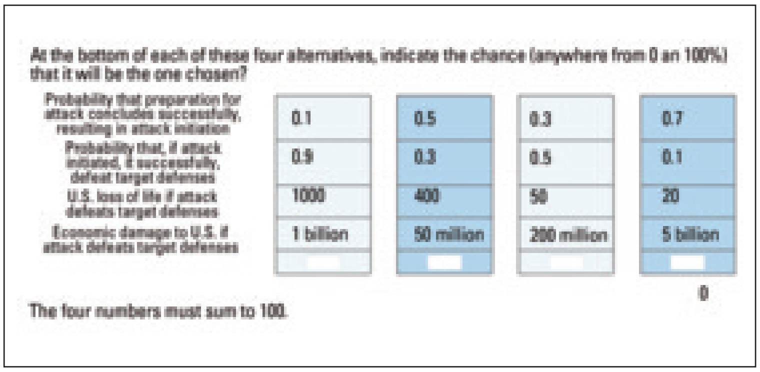
Modelling threat from goal-oriented, adaptive adversaries is fundamentally different from modelling potential hazards associated with forces of nature. Adversaries evaluate potential attacks based on criteria that are important to them and then choose the attack which suits their objectives best. When the adversary decision criteria change, their choice may change as well. Unlike consequence or vulnerability estimates, a threat estimate for an attack scenario depends not only on the characteristics of that scenario, but on the characteristics of all attack scenarios that the adversary is choosing from.

To account for these concepts, the CRM-D includes a 'probabilistic adversary decision model' (PADM), which is composed of two sub-models: the 'adversary value model' (AVM) and the 'attack choice model' (ACM). The decision model is probabilistic because no aspect of the adversary's future decision process can be known with certainty.

### Adversary value model

This quantifies expert judgement about how adversaries evaluate the relative attractiveness of attack scenarios, based on the scenarios' characteristics that the adversary is likely to take into account. These features, related to the adversary capabilities and intent, reflect the various expected benefits, costs, and risks associated with each attack scenario. The adversary value model also quantifies the underlying uncertainty about the value system, which stems from the differences of opinion among experts and the uncertainty of each individual expert about the attacker value system.

To model the attack scenario evaluation process followed by an adversary, it is first necessary to identify the adversarial goals driving the selection of a particular attack scenario. For the type of adversary under consideration (highly capable, transnational terrorist organization), this was conducted through literature review and interviews with selected groups of terrorism experts from various government and research organizations. It was found that an ideal attack for these adversaries would cause grave physi-



At the bottom of each of these four alternatives, indicate the chance (anywhere from 0 an 100%) that it will be the one chosen?

| | | | | |
|---|---|---|---|---|
| Probability that preparation for attack concludes successfully, resulting in attack initiation | 0.1 | 0.5 | 0.3 | 0.7 |
| Probability that, if attack initiated, it successfully, defeat target defenses | 0.9 | 0.3 | 0.5 | 0.1 |
| U.S. loss of life if attack defeats target defenses | 1000 | 400 | 50 | 20 |
| Economic damage to U.S. if attack defeats target defenses | 1 billion | 50 million | 200 million | 5 billion |
| | | | | |

0

The four numbers must sum to 100.

*Fig. 2. Example of a set of hypothetical attack alternatives.*

cal and psychological damage while having a relatively low chance of failure [Ackerman *et al*., 2007[5]; Davis *et al*., 2009[6]; Libicki *et al*., 2007[7]].

Based on the assumed goals, the following variables were identified as the controlling factors influencing the attack scenario evaluation process from the adversary's perspective:

- adversary's perception of the probability of successfully defeating the national and local defensive layers;
- adversary's perception of the probability of successfully defeating the target defensive layers, given success against the national and local defences;
- adversary's perception of the expected level of consequences in terms of the loss of life resulting from a successful attack; and,
- adversary's perception of the expected level of consequences in terms of the economic impacts resulting from a successful attack.

These key variables, the quantification of which is relatively straightforward, were selected from a larger set of variables identified as potentially relevant for attack scenario evaluation purposes. For example, according to background research, the adversary was deemed to value spectacular attacks on iconic targets. However, how spectacular an attack might be is not easily quantifiable, and iconicity is only considered when it varies across targets in a portfolio. In addition, an event deemed as spectacular may exhibit a strong correlation with loss of life and economic damage, and therefore it may be captured by the key variables selected above.

A comprehensive expert elicitation was conducted with participation of representatives from multiple federal agencies, owners and operators, state fusion centres, and other state agencies responsible for law enforcement and public safety. The elicitation was conducted using a self-paced, interactive, online interview process using the Sawtooth software for conjoint (trade-off) analysis [Orme, 2010[8]].

In the main elicitation task, each SME was presented with 10 or 20 different sets of four hypothetical attack options. The options were created by systematically varying the values of the key attack features in a way that makes a statistical estimation of the adversary's value system more efficient. For each set of options, each expert was asked to provide the probability that each of the options in the set would be chosen by adversaries, given that one of them would be chosen. Eliciting probabilities provides a way of incorporating each SME's uncertainty. Fig. 2 shows an example of one of the sets of hypothetical attack options used in the elicitation.

Statistical modelling provides a way of aggregating the judgements of individual SMEs into a cumulative judgement, and of quantifying the trade-offs the SMEs believe the adversaries would make among the different attack features. It also quantifies uncertainty about the value system, which stems from SME uncertainty and differences of opinion. Estimating the value system involves running a regression, where the dependent variable is the expert's judgement about an attack alternative, and the independent variables are values of the features of the corresponding attack option. The regression is a version of conditional logit (a regression model appropriate when the data reflects choices among options) which is modified to analyse probabilistic choice data [Blass *et al*., 2010[9]; Kirpichevsky *et al*., 2012[10]].

The adversary value system takes the form of a functional relationship among the key decision variables, which is chosen to best fit the elicited data. The effect of each of the variables on the value assigned by the adversary to attack scenarios (utility) was found to have a concave pattern: increases at the lower end of the variable ranges result in greater utility increases. This indicates decision-making consistent with thresholding: for example, once a certain level of probability of success or consequences can be expected, scenario attractiveness does not change much, whereas change is significant below the threshold. This is consistent with the narrative answers provided by SMEs during the elicitation. In those answers, SMEs also stressed that the most important decision criterion for the adversary was aversion to failure, and that loss of life was the more important of the two consequence variables, which was reflected in the estimated value system[*].

## Attack choice model

The attack choice model uses the estimated adversary value system to calculate P(A) for any set of attack scenarios and to carry out ROI analyses for risk mitigation options. To make the P(A) calculation possible, attack scenarios in the portfolio need to be formulated in terms that the adversary value model can accommodate. This involves using the CRM-D consequence and vulnerability models to estimate the values for loss of life, total economic impacts, and the probabilities of defeating the national/local and target defences for every scenario in the portfolio. These variables are used as proxies for the adversary perceptions of these variables.

The attack choice model then uses the estimated adversary value function and the uncertainty around it to simulate the possible utility values for a set of attack scenarios. The current CRM-D assumption is that the

*For example, suppose scenario consequences in terms of loss of life and economic damage are equal to 10 and $10 million respectively, and the combined P(S|A) is equal to 0.2. If P(S|A) were to drop to 0.1, it would require an offsetting increase in consequences equal to either 400 lives or $2.5 billion, for the adversary to retain roughly the same overall utility for the scenario.

**If the adversary believes that risk mitigation might involve deception or randomization, they might not necessarily choose a scenario that is perceived to have the highest value. A game theory module is under development to address this issue.

***Because P(A) is conditional on attack within a portfolio, deterrence is not modelled, in response to risk mitigation, the P(A) can only shift among the scenarios, and the sum of P(A) will always be no less than 1. Future work on the AVM elicitation will enable estimating the deterrence effect of investments.

adversary selects the attack scenario perceived to have the highest value, and so P(A) for an attack scenario is calculated as the fraction of the simulations, in which the scenario has the highest value in the set(**).

Because CRM-D models adversaries as adaptive decision-makers, it is important to note that some risk mitigation investments may decrease P(A) for some scenarios, while causing an increase for other scenarios(***). Therefore, it is theoretically possible for an investment aimed at risk mitigation actually to increase the portfolio risk if the threat shifts to attack scenarios which pose more risk. Risk managers should be mindful of the complex interactions associated with the target selection process used by adaptive adversaries.

## Pilot implementation at USACE projects

In 2011, the USACE initiated a pilot implementation of the CRM-D at selected of dam and navigation lock projects in the USACE Northwestern Division (Columbia river, Willamette river tributary, and Missouri river basins), Mississippi Valley Division (Mississippi river basin), and Great Lakes and Ohio River Division (Ohio river basin). Each project had unique features, functions, and operational conditions which offered ideal conditions to test the capabilities of the methodology and its applicability to a large portfolio.

Risk was estimated in terms of expected loss of life and total economic damage for 16 attack scenarios associated with nine dams and two attack vectors. Fig. 3 shows the product of P(A) and P(S|A) plotted against economic consequences for attack scenarios (the targets are indexed by letters, and the attack vectors by numbers). Thus, risk in terms of economic consequences could be determined by multiplying the two coordinates together.

Fig. 3 shows iso-curves that could represent thresholds of risk as determined by a decision-maker, for example, a portfolio owner. The curves trace those points for which risk is greater than $50 million (above the red line), and greater than $20 million (above the green line). Decision makers could hypothetically use such information to identify more readily those dams that they choose to focus on for developing investment options. The risk values that would define these curves could be chosen in accordance with decision makers' priorities.

A portfolio risk manager might wish to assess an impact of a particular investment on risk. For example, the addition of K12-rated vehicle barriers at seven of the projects where they had not been previously installed at a total cost of less than $1 million could reduce portfolio risk given attack by $66 million in expected economic damage and 34 lives. To decide whether this is a worthy investment, a risk manager would have to assume or elicit from SMEs a predicted annual frequency of attacks in the portfolio and then use it to compare this and other investments with the time-discounted values of the resulting risk reductions.

## Conclusion

The Common Risk Model for Dams (CRM-D) is a consistent, mathematically rigorous, and easy to implement method for security risk assessment of dams, navigation locks, hydro projects, and similar infrastructure. This methodology, the result of collaborative efforts between the US Army Corps of Engineers and the US Department of Homeland Security, provides a systematic approach for evaluating and comparing security risks across a large portfolio. ◊

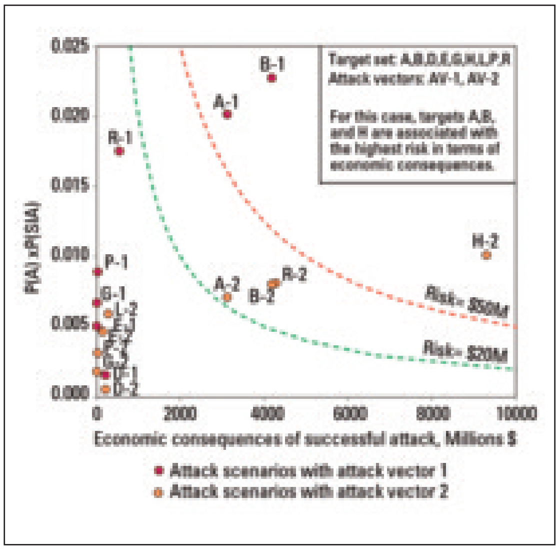


*Fig. 3. Scenarios by economic consequences of success and probability of success.*

## References

1. **Seda-Sanabria, Y., Fainberg, M.A., and Matheu, E.E.,** "A Consistent Approach for Vulnerability Assessment of Dams," *Proceedings*, 31st US Society of Dams Annual Meeting and Conference, San Diego, California, USA; 2011.
2. **Cox Jr, L.A.,** "Some Limitations of "Risk = Threat × Vulnerability × Consequence" for Risk Analysis of Terrorist Attacks," *Risk Analysis*, Vol. 28, No. 6; 2008.
3. **Seda-Sanabria, Y., Fainberg, M.A., Matheu, E. E., Tressler, J. D., and Bowen, M. L.,** "Implementation of the Common Risk Model for Dams for Security Assessments of USACE Critical Infrastructure," *Proceedings*, Dam Safety 2011 Conference, Washington, DC, USA; 2011.
4. **Morgeson, J.D., Seda-Sanabria, Y., Matheu, E.E. and Keleher, M.J.,** "Incorporating Uncertainties in the Estimation of Vulnerabilities for Security Risk Assessments," *Proceedings*, 33rd US Society of Dams Annual Meeting and Conference, Phoenix, Arizona, USA; 2013.
5. **Ackerman, G., Abhayaratne, P., Bale, J., Bhattacharjee, A., Blair, C., Hansell, L., Jayne, A., Kosal, M., Lucas, S., Moran, K., Seroki, L., and Vadlamudi, S.,** "Assessing Terrorist Motivations for Attacking Critical Infrastructure," UCRL-TR-227068, Center for Nonproliferation Studies, Laurence Livermore National Laboratory, 2007.
6. **Davis, P. K. and Cragin, K.,** (Eds.) "Social Science for Counterterrorism: Putting the Pieces Together," Rand Monograph; 2009.
7. **Libicki, M.C., Chalk, P., and Sisson, M.,** "Exploring Terrorist Targeting Preferences," Rand Monograph; 2007.
8. **Orme, B.K.,** "Getting Started with Conjoint Analysis", Research Publishers LLC, Madison, Wisconsin, USA; 2010.
9. **Blass, A.A., Lach, S. and Manski, C.F.,** "Using Elicited Choice Probabilities to Estimate Random Utility Models: Preferences for Electricity Reliability," *International Economic Review*, Vol. 51, No. 2; May 2010.
10. **Kirpichevsky et al.,** "Estimating Threat from Adaptive Adversaries: Probabilistic Decision Modeling in the CRM-D", Draft Paper, Institute for Defense Analyses, Alexandria, VA, USA; May 2012.

## Bibliography

**Dechant, J., et al.,** "The common risk model for dams: Methodology and application", IDA Paper P-4761, Institute for Defense Analyses, Alexandria, VA, USA; April 2012.

*Y. Seda-Sanabria*

*E. Matheu*

*J.D. Morgeson*

*Y. Kirpichevsky*

*M.A. Fainberg*

*J.A. Dechant*

*V.A. Utgoff*

**Ms Yazmin Seda-Sanabria** serves as the National Program Manager of the Critical Infrastructure Protection and Resilience Program, Office of Homeland Security, US Army Corps of Engineers, Headquarters. She leads policy, technical guidance, and supervision of the development and implementation of a national risk management strategy for the protection, security, and improved resilience of USACE's civil works portfolio of critical dams, navigation locks, and hydro facilities. She holds BS and MS degrees in Civil Engineering from the University of Puerto Rico at Mayagüez, and a second MS degree in Engineering Mechanics from the Mississippi State University, USA.

Critical Infrastructure Protection and Resilience Program, Office of Homeland Security, US Army Corps of Engineers, Headquarters, Washington, DC 20314, USA.

**Dr. Enrique Matheu** serves as Chief of the Critical Lifelines Branch in the Sector Outreach and Programs Division, Office of Infrastructure Protection, National Protection Programs Directorate, US Department of Homeland Security. Dr Matheu leads the national programme for development, implementation, and coordination of risk management activities conducted under a voluntary partnership framework, aimed at improving the security and resilience of dams, levees, hydropower projects, and nuclear facilities as important components of the critical infrastructure in the USA. Dr Matheu holds a BS degree in Civil Engineering from the National University of Córdoba, Argentina, an MS degree in Civil Engineering from the University of Puerto Rico at Mayagüez, and a PhD in Engineering Mechanics from the Virginia Polytechnic Institute and State University, USA.

Critical Lifelines Branch, Office of Infrastructure Protection, National Protection and Programs Directorate, Department of Homeland Security, Washington, DC 20598, USA.

**J. Darrell Morgeson** graduated from West Point in 1971 and earned his Master's Degree in Operations Research from the Naval Post Graduate School in 1981. Following 13 years in the active duty in the Army, he spent 18 years at Los Alamos National Laboratory, focusing the last few years on simulations of US critical infrastructure. From 2001 until 2003, he served in the Office of Homeland Security in the White House as the Director of Critical Infrastructure Protection. He has spent the last 10 years focusing on developing risk models and analyses on the nation's critical infrastructure.

**Dr Yevgeniy Kirpichevsky** graduated from the University of Illinois at Urbana-Champaign, USA, with degrees in Finance and Political Science, in 2001. He received his PhD in Government from Harvard University in 2009. As a research analyst at the Institute for Defense Analyses, he has applied statistical and mathematical modelling to various problems in national security, including terrorism risk analysis and nuclear deterrence.

**Dr M. Anthony Fainberg** earned his PhD in Elementary Particle Physics from the University of California, Berkeley, USA, in 1969. After 12 years in basic research, he changed fields to focus on areas where national security and science intersect. He has worked for national laboratories and the US Government in areas including nuclear non-proliferation, aviation security, nuclear smuggling, and counter terrorism. For the past eight years, he been a staff member at the Institute for Defense Analyses, working on risk methodologies related to the protection of the nation's critical infrastructure.

**Dr Jason A. Dechant** graduated from Kansas State University in 1997 and earned his Master's degree in Diplomacy and International Commerce from the University of Kentucky, USA, in 1999. He later received his PhD in Public Policy from George Mason University, USA. Since January 2000, Dr Dechant has been on the research staff at the Institute for Defense Analyses, specializing in resource management, strategic planning, and risk assessment. From 2001 until 2004, he served in the Office of the Under Secretary of Defense for Policy in the Pentagon as a Special Assistant for Strategy. Since 2009, Dr Dechant has been involved with developing and implementing risk assessment methods for critical infrastructure and defense resource decision-making.

**Dr Victor A. Utgoff** is a graduate of the Massachusetts Institute of Technology, and earned a PhD in Electrical Engineering from Purdue University. Until mid-2007, he was a Deputy Director of the Strategy, Forces, and Resources Division at the Institute for Defense Analyses (IDA). From 1977 to 1981, Dr Utgoff was a senior member of the National Security Council Staff. Prior to those assignments he worked for various research and aerospace organizations. Since 2002, he has worked on a series of counter-terrorism studies, mostly developing analytical methods to support decision-making on investments to protect critical infrastructure. In 1999, he received IDA's Andrew J. Goodpaster Award for Excellence in Research.

Strategy, Forces and Resources Division, Institute for Defense Analysis, Alexandria, Virginia 22311, USA.

| | |
|---|---|
| **REPORT DOCUMENTATION PAGE** | *Form Approved*<br>*OMB No. 0704-0188* |

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

| | | |
|---|---|---|
| **1. REPORT DATE (DD-MM-YY)**<br>June 2013 | **2. REPORT TYPE**<br>Final | **3. DATES COVERED (From – To)** |
| **4. TITLE AND SUBTITLE**<br>The Common Risk Model for Dams: A Portfolio Approach to Security Risk Assessments | | **5a. CONTRACT NO.**<br>DASW01-04-C-0003<br>**5b. GRANT NO.**<br>**5c. PROGRAM ELEMENT NO(S).** |
| **6. AUTHOR(S)**<br>Yev Kirpichevsky, Yazmin Seda-Sanabria, Enrique E. Matheu, Jason A. Dechant, M. Anthony Fainberg, J. Darrell Morgeson, Victor A. Utgoff | | **5d. PROJECT NO.**<br>**5e. TASK NO.**<br>BA-6-3075<br>**5f. WORK UNIT NO.** |
| **7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**<br>Institute for Defense Analyses<br>4850 Mark Center Drive<br>Alexandria, VA 22311-1882 | | **8. PERFORMING ORGANIZATION REPORT NO.**<br>IDA NS Document D-4943 |
| **9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)**<br>Critical Infrastructure Protection & Resilience (CIPR) Program<br>U.S. Army Corps of Engineers Headquarters<br>Office of Homeland Security<br>441 G Street NW<br>Washington, DC 20314-1000 | | **10. SPONSOR'S / MONITOR'S ACRONYM(S)**<br>**11. SPONSOR'S / MONITOR'S REPORT NO(S).** |

**12. DISTRIBUTION / AVAILABILITY STATEMENT**

Approved for public release; distribution is unlimited.

**13. SUPPLEMENTARY NOTES**

**14. ABSTRACT**

The Common Risk Model for Dams (CRM-D) is a consistent, mathematically rigorous, and easy to implement method for security risk assessment of dams, navigation locks, hydropower projects, and similar infrastructures. The methodology provides a systematic approach for evaluating and comparing security risks across a large portfolio. Risk is calculated for attack scenarios (specific adversary using a specific attack vector against a specific target) by combining consequence, vulnerability, and threat estimates in a way that properly accounts for the relationships among these variables. The CRM-D can effectively quantify the benefits of implementing a particular risk mitigation strategy and, consequently, enable return-on-investment analyses for multiple mitigation alternatives across a large portfolio.

**15. SUBJECT TERMS**

Risk Assessment, Common Risk Model, Dams Sector, Homeland Security, Portfolio Analysis

| **16. SECURITY CLASSIFICATION OF:** | | | **17. LIMITATION OF ABSTRACT** | **18. NO. OF PAGES** | **19a. NAME OF RESPONSIBLE PERSON**<br>Jason A. Dechant |
|---|---|---|---|---|---|
| **a. REPORT**<br>U | **b. ABSTRACT**<br>U | **c. THIS PAGE**<br>U | UU | 10 | **19b. TELEPHONE NUMBER (Include Area Code)**<br>703-845-2489 |